

In the Claims:

Amend the claims as follows:

5

1. (Currently amended) ~~Method A method~~ for secure forwarding of a message from a first computer to a second computer via an intermediate computer in a telecommunication network, ~~characterized by comprising:~~
- 10 ~~characterized by comprising:~~
- a) forming a message in the first computer or in a computer that is served by the first computer, and in the latter case sending the message to the first computer,
- b) in the first computer, forming a secure message by giving
- 15 the message a unique identity and a destination address,
- c) sending the secure message from the first computer to the intermediate computer,
- d) using said destination address and the unique identity to find an address to the second computer,
- 20 e) substituting the current destination address with the found address to the second computer,
- f) substituting the unique identity with another unique identity, and
- g) forwarding the secure message with substituted current
- 25 destination address and substituted unique identity to the second computer.
2. (Currently amended) ~~Method of claim 1, characterized in that~~ The method of claim 1 wherein the method
- 30 further comprises forming the secure message is formed in step b) by using an IPsec connection between the first computer and the second computer ~~formed for this purpose in the method.~~
- 35 3. (Currently amended) ~~Method of claim 1, characterized~~

~~z-e-d in that~~ The method of claim 1 wherein the method further comprises performing a the secure forwarding of the message ~~is performed~~ by making use of the SSL or TLS protocols.

5

4. (Currently amended) ~~Method of claim 2, characterized in that~~ The method of claim 2 wherein the method further comprises manually performing a preceding distribution of keys to the components for forming the IPsec connection ~~is performed manually.~~

10

5. (Currently amended) ~~Method of claim 2, characterized in that~~ The method of claim 2 wherein the method further comprises performing a preceding distribution of keys for forming the IPsec connection ~~is performed~~ by an automated key exchange protocol.

15

6. (Currently amended) ~~Method of claim 5, characterized in that~~ The method of claim 5 wherein the method further comprises performing the automated key exchange protocol used for the preceding distribution of keys for forming the IP Sec connection is performed by means of a modified IKE key exchange protocol between the first computer and the intermediate computer and by means of a standard IKE key exchange protocol between the intermediate computer and the second computer.

20

25

7. (Currently amended) ~~Method of any of claims 2, 5 or 6, characterized in that~~ The method of claim 2 wherein the method further comprises sending the message that is sent from the first computer in step c) is as a packet and that contains message data, an inner IP header containing the actual sender and receiver addresses, an outer IP header containing the addresses of the first computer and the intermediate computer, the unique identity, and other

30

35

~~security parameters.~~

8. (Currently amended) ~~Method of any of claims 2, 5 or 6, c h~~
~~a r a c t e r i z e d i n t h a t~~ The method of claim 1 wherein
5 the method further comprises ~~that~~ the IPSec connection is
being one or more security associations (SA) and the unique
identity is being one or more SPI values ~~and the other~~
~~security parameters include one or more sequence numbers.~~
- 10 9. (Currently amended) ~~Method of any of claims 1 - 8, c h a r~~
~~a c t e r i z e d i n t h a t~~ The method of claim 1 wherein the
method further comprises performing the matching in step d)
is performed by using a translation table stored at the
intermediate computer.
- 15 10. (Currently amended) ~~Method of any of claims 1 - 9, c h a~~
~~r a c t e r i z e d i n t h a t~~ The method of claim 1 wherein
the method further comprises changing both the address and
the SPI-value ~~are changed~~ by the intermediate computer in
20 steps e) respective and f).
11. (Currently amended) ~~Method of any of claims 1 - 10, c h a~~
~~r a c t e r i z e d i n t h a t~~ The method of claim 1 wherein
the method further comprises the first computer is being a
25 mobile terminal, whereby so that the mobility is enabled by
modifying the translation table at the intermediate
computer.
12. (Currently amended) ~~Method of claim 11, c h a r a c t e r~~
~~i z e d i n t h a t~~ The method of claim 11 wherein the method
30 further comprises performing the said modification of the
translation tables is performed by sending a request for
registration of the new address from the first computer to
the intermediate computer.

35

BEST AVAILABLE COPY

13. (Currently amended) ~~Method of claim 12, characterized~~
in that The method of claim 12 wherein the method
further comprises sending a reply to said the request for
registration is sent from the intermediate computer to the
5 first computer.
14. (Currently amended) ~~Method of claim 12 or 13, characterized~~
in that The method of claim 12 wherein the
method further comprises authenticating or encrypting by
10 IPSec the request for registration and/or reply is
authenticated and/or encrypted by IPSec.
15. (Currently amended) ~~Method of any of claims 4-14, characterized~~
in that The method of claim 4 wherein
15 the method further comprises establishing the key
distribution for the secure connections is established by
establishing an IKE protocol translation table, and using
the translation table to modify IP addresses and cookie
values of IKE packets in the intermediate computer.
20
16. (Currently amended) ~~Method of claim 15, characterized~~
in that The method of claim 15 wherein the method
further comprises establishing the key exchange
distribution is established by
25 generating an initiator cookie and sending a zero responder
cookie to the second computer,
generating a responder cookie in the second computer,
establishing a mapping between IP addresses and IKE cookie
values in the intermediate computer, and
30 using the translation table to modify IKE packets in flight
by modifying the external IP addresses and possibly IKE
cookies of the IKE packets.
17. (Currently amended) ~~Method of claim 15 or 16, characterized~~
35 in that The method of claim 15 wherein the

BEST AVAILABLE COPY

method further comprises modifying the modified IKE protocol between the first computer and the intermediate computer ~~is modified~~ by transmitting the IKE keys from the first computer to the intermediate computer in order to decrypt and ~~modificate~~ modify IKE packets.

18. (Currently amended) ~~Method of claim 15 or 16, characterized in that~~ The method of claim 15 wherein the method further comprises carrying out in the modified IKE protocol between the first computer and the intermediate computer the modification of the IKE packets ~~is done~~ by the first computer with the intermediate computer requesting such modifications.

19. (Currently amended) ~~Method of claim 17, characterized in that~~ The method of claim 17 wherein the method further comprises defining the address ~~is defined~~ so that the first computer is identified for the second computer by the intermediate computer by means of an IP address taken from a pool of user IP addresses when forming the translation table.

20. (Currently amended) ~~Method of any of claims 1-19, characterized in that~~ The method of claim 1 wherein the method further comprises sending the secure message ~~is sent~~ by using an IPSec transport mode.

21. (Currently amended) ~~Method of any of claims 1-19, characterized in that~~ The method of claim 1 wherein the method further comprises sending the secure message ~~is sent~~ by using an IPSec tunnel mode.

22. (Currently amended) ~~Telecommunication~~ A telecommunication network for secure forwarding of messages, comprising:
at least a first computer, a second computer and an

intermediate computer,

~~characterized in that~~

the first and the second computers have means to perform having means for performing an IPSec processing, and

5 the intermediate computer have having translation tables to perform IPSec and IKE translation.

23. (Currently amended) ~~Network of claim 22, characterized in that~~ The telecommunication network of claim
10 22 wherein the translation table for IPSec translation ~~comprises~~ has IP addresses of the intermediate computer to be matched with IP addresses of the second computer.

24. (Currently amended) ~~Network of claim 22, characterized in that~~ The telecommunication network of claim
15 22 wherein the translation tables for IKE translation consists of two partitions, one for the communication between the first computer and the intermediate computer and another for the communication between the intermediate
20 computer and the second computer.

25. (Currently amended) ~~Network of claim 24, characterized in that~~ The telecommunication network of claim
25 24 wherein both partitions of the mapping table for IKE translation contains translation fields for a source IP address, a destination IP address, initiator and responder cookies between respective computers.

26. (Currently amended) ~~Network of any of claims 22 - 25, characterized in that~~ The telecommunication
30 network of claim 22 wherein there is another translation table for IKE translation containing fields for matching a given user to a given second computer.